RFC-0011 FedRAMP Pilot Standard for Storing and Sharing Authorization Data

Friday, May 23, 2025

Background

The FedRAMP Authorization Act (44 USC § 3609 (a) (8)) directs the Administrator of the General Services Administration to *"provide a secure mechanism for storing and sharing necessary data, including FedRAMP authorization packages, to enable better reuse of such packages across agencies, including making available any information and data necessary for agencies…"* This responsibility is delegated to the FedRAMP Director.

Oxford Languages defines a mechanism as *"a natural or established process by which something takes place or is brought about."*

OMB Memorandum M-24-15 on Modernizing FedRAMP section 6 states that *"In general, to encourage both security and agility, Federal agencies should use the same infrastructure relied on by the rest of CSPs' commercial customer base."*

Introduction

The FedRAMP Pilot Standard for Storing and Sharing Authorization Data defines requirements for cloud service providers to store and share authorization data with federal agencies using their existing commercial processes and trust centers. This standard provides a secure mechanism to enable better reuse of authorization data

across agencies and to make all necessary information and data available to agencies.

This standard will initially be implemented as an opt-in pilot open to cloud service providers, allowing FedRAMP, providers, and agencies to learn directly how to best implement and adopt an effective shared responsibility model for storing and sharing authorization data. Providers who establish trust centers that meet these requirements, as verified by FedRAMP, will be exempted from FedRAMP requirements to share materials via the FedRAMP Secure Repository on the USDA Connect Community Portal or existing secure repositories. Please note that explicit requirements during the pilot may vary slightly from the draft standard.

Cloud service providers MAY continue to rely on the FedRAMP secure repository they currently use for sharing information with agencies during the pilot and any following transition period. Providers SHOULD monitor the pilot as the existing FedRAMP Secure Repository and related mechanisms will likely be replaced with this model during FY26 (or earlier).

FedRAMP Trust Center Requirements

Cloud service providers SHOULD establish a trust center or similar centralized location to make security information and materials (“authorization data”) available to stakeholders.

1. The FedRAMP trust center MUST be highly visible on a provider’s core website and MUST clearly state that it includes FedRAMP related materials. The FedRAMP related section SHOULD be available via a direct link that can be included in the FedRAMP marketplace.
2. The FedRAMP trust center MUST publicly share the following information about the cloud service offering:
    a. Direct link to the FedRAMP Marketplace for the offering

RFC-0017

   b. Description of the services offered within the FedRAMP authorization scope

   c. Information for requesting access to non-public FedRAMP materials

3. The FedRAMP trust center MUST store additional information about the cloud service offering that MAY not be available publicly based on a risk assessment by the cloud service provider. This information MAY be available to the public and MUST be available to federal agencies upon request, including:

   a. Security Plans and Appendices

   b. Assessments and Authorizations, including supporting artifacts

   c. Continuous Monitoring reporting/documentation and supporting artifacts

   d. Plan Of Action And Milestones (POA&M)

   e. Significant Change Notifications (SCN)

   f. Incident Reports

   g. Listing of other FedRAMP authorized services being leveraged

   h. Any other authorization data required by FedRAMP

4. The FedRAMP trust center MUST provide a well-documented API or similar machine access to authorization data for federal agencies.

5. Providers MUST make authorization data available in both human-readable and machine-readable formats.

6. Providers migrating from the FedRAMP Secure Repository on the USDA Connect Community Portal MUST provide migration information for agencies in their secure folder.

7. Providers SHOULD follow FedRAMP's best practices and technical assistance on storing and sharing authorization data where applicable.

RFC-0017

Provider Access Responsibilities

Cloud service providers are entirely responsible for the intellectual property stored in their FedRAMP trust centers and MUST manage all access to the authorization data stored in their trust centers.

1. Providers MUST publicly provide plain-language policies and guidance for federal government customers to follow to obtain and manage access to authorization data stored by the cloud service provider.
2. Providers MUST grant FedRAMP full access to all authorization data. This MUST include reasonable API access and a secure mechanism to routinely manage API credentials.
3. Providers MUST grant agency authorizing officials (and/or their delegates) full access to all authorization data if they have active customer agreements or indirectly use the service. This MUST include reasonable API access and a secure mechanism to routinely manage API credentials.
4. Providers SHOULD NOT store federal information that is within the FedRAMP Minimum Assessment Scope within the trust center; providers MUST limit access to such information according to the owner of that federal information.
5. Providers SHOULD include standard mechanisms that allow customers to manage authorization data access for their users and services directly; these mechanisms SHOULD be the same that customers use to manage access to other aspects of the cloud service offering.
6. Providers SHOULD grant agency Authorizing Officials and/or their delegates without an active customer agreement temporary full access to all authorization data as appropriate if an agency is directly or indirectly considering use of the system.
7. Providers SHOULD follow FedRAMP best practices and technical assistance related to storing and sharing authorization data as appropriate.

RFC-0017

Agency Request Responsibilities

Agencies SHOULD use native mechanisms provided by cloud service offerings to manage their own user and/or service access to authorization data.

If such mechanisms are unavailable, agencies SHOULD follow the request process identified in the FedRAMP Marketplace for a specific cloud service offering to request access to authorization data for review.

In all cases:

1. Agencies MUST limit access of employees and services to non-public authorization data to employees and services with an explicit need for access.
2. Agencies MUST limit distribution of non-public authorization data to that required for agency operations and delete data after it is no longer needed.
3. Agencies SHOULD follow FedRAMP best practices and technical assistance related to storing and sharing authorization data as appropriate.

RFC-0017